|  |  |
| --- | --- |
|  | 2.pielikums pie atklāta konkursa  Nr. RD IKSD 2021/3 nolikuma 1.pielikuma “Tehniskā specifikācija” |

**Pasākumi, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumi un mehānismi, ar ko nodrošina personas datu aizsardzību (Veidlapas paraugs)**

Izpildītājam jāaizpilda neiekrāsotie lauki, ciktāl tas attiecas uz datu apstrādi E-žurnāla sistēmā.

|  |  |  |
| --- | --- | --- |
| **Jautājumi** | **Atbildes** | **IT drošības pārvaldnieka un datu aizsardzības speciālista (ja nepieciešams) viedoklis** |
| 1. Vai ir noteikta atbildīgā persona, kas uzrauga informācijas un komunikācijas tehnoloģiju sistēmas izstrādi, ieviešanu un uzturēšanas ārpakalpojuma līguma izpildi? |  | *Šo kolonu aizpilda Datu aizsardzības un informācijas tehnoloģiju drošības centra darbinieki.* |
| 1. Kādi resursi[[1]](#footnote-2), tīkla protokoli un porti, tīkla un tīklam pieslēgto iekārtu identifikācijas un konfigurācijas parametri, cilvēkresursi, papīra dokumenti, papīra dokumentu vai papīra dokumentu aprites kanāli, u.c.) tiks izmantoti Projektā? |  |  |
| 1. Vai ir noteiktas informācijas resursu jeb personas datu apstrādes prasības Projektā? |  |  |
| 1. Vai neplānots personas datu apstrādes pieejamības pārtraukums drīkstēs būt lielāks par četrām stundām mēnesī darba laikā (summāri)? Pamatojiet atbildi. |  |  |
| 1. Vai personas datu integritātes apdraudējums var radīt risku valsts un pašvaldību institūcijas pamatfunkciju nodrošināšanai? Pamatojiet atbildi. |  |  |
| 1. Vai personas datu neatļauta izpaušana vai noplūde var radīt smagākas sekas nekā kaitējums valsts un pašvaldību institūcijas, citu institūciju vai Latvijas Republikas reputācijai? Pamatojiet atbildi. |  |  |
| 1. Vai atbildīgā persona par informācijas resursiem ir identificējusi:    1. maksimāli pieņemamo personas datu atjaunošanas ilgumu (RTO)?    2. maksimāli pieņemamo personas datu zudumu, atjaunojot tos no rezerves kopijas? | 7.1.  7.2. |  |
| 1. Vai un kādā kārtībā personas, kas piekļūs personas datiem informēs par pienākumu neizpaust personas datus (tostarp pēc darba, dienesta vai citu tiesisko attiecību izbeigšanās)? Kā tiks kontrolēta šā pienākuma ievērošana? |  |  |
| 1. Atbildīgais par informācijas sistēmas (Projekta) drošību. Norādiet amatu/ārpakalpojuma sniedzēju, kas nodrošina un atbild par informācijas pieejamības, integritātes un konfidencialitātes nodrošināšanu. |  |  |
| 1. Šifrēšana    1. Vai tiks veikta šifrēšana?[[2]](#footnote-3) Aprakstiet apstrādes procesā ieviestās un izmantotos šifrēšanas līdzekļus (VPN, TLS, utt).    2. Ja ierobežotas pieejamības informācija atradīsies ārpus pašvaldības kontrolē esošiem resursiem, vai tiks nodrošināta nepieciešamā loģiskā aizsardzība (piemēram, šifrēšana u.c.)? Ja jā, sniedziet informāciju par to. | 10.1.  10.2. |  |
| 1. Anonimizēšana. Vai tiks ieviesta datu anonimizēšana, kāda un kādam mērķim? Neaizmirstiet skaidri nošķirt anonimizētus un pseidonimizētus datus. Sīkāk sk. 29.panta darba grupas vadlīnijas.[[3]](#footnote-4) |  |  |
| 1. Pseidonimizācija[[4]](#footnote-5). Vai tiks ieviesta datu pseidonimizēšana? |  |  |
| 1. Personas datu nodalīšana.[[5]](#footnote-6) Vai tāda tiks ieviesta? |  |  |
| 1. Vai ir noteiktas resursu darbspēju uzturēšanas prasības? |  |  |
| 1. Loģiskās piekļuves kontroles[[6]](#footnote-7).    1. Norādiet vai ir izstrādātas informācijas sistēmu piekļuves kontroles procedūras?    2. Vai ir noteikta kārtībā, kādā pārvalda lietotāju piekļuves tiesību pieprasījumus un lietotāja piekļuves tiesību piešķiršanas pārvaldību kopumā?    3. Raksturojiet kā pārvaldiet/pārvaldīsiet informācijas sistēmu lietotāju kontus.    4. Vai ir noteiktas piekļuves tiesību lomas un to tiesības? Ja jā, sniedziet informāciju par to. | 15.1.  15.2.  15.3.  15.4. |  |
| 1. Priviliģētie lietotāji.    1. Vai ir noteikta priviliģētā lietotāja tiesību piešķiršanas pārvaldības kārtība Projektā? Ja jā, sniedziet informāciju par to.    2. Kuru iestāžu/struktūrvienību/ārpakalpojumu sniedzēju darbiniekiem ir/tiks piešķirtas priviliģēto lietotāju tiesības Projektā?    3. Vai attiecīgā Projekta administrēšanas darbu izpildē tiek izmantoti atsevišķi unikāli lietotāja konti, kas nesakrīt ne ar vienu citu esošu lietotāja kontu (identifikatoru), un kas netiek izmantots ikdienas darbu (kas nav saistīti ar administrēšanas darbiem) izpildē?    4. Vai ir nodrošināts, ka Projektā attiecīgā resursa/sistēmas administrēšanas darbus veic priviliģētais lietotājs, izmantojot īpašu priviliģētā lietotāja kontu?    5. Vai Projektā ikviens lietotāja konts ir saistīts ar konkrētu fizisko personu?    6. Vai Projektā jebkura piekļuve sistēmai ir izsekojama līdz konkrētam lietotāja kontam vai interneta protokola (IP) adresei? | 16.1.  16.2.  16.3.  16.4.  16.5. |  |
| 1. Vai tiks nodrošināta sistēmas drošību ietekmējošu apdraudējumu atklāšana, uzskaite, vērtēšana Projektā? |  |  |
| 1. Paroles.    1. Vai lietotāja paroles garums ir vismaz deviņi simboli un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu vai speciālu simbolu?    2. Vai ir pieļauta funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada?    3. Vai infrastruktūras iekārtās, kas nodrošina sistēmas funkcionēšanu, ir nomainītas noklusējuma iekārtu ražotāja vai izplatītāja uzstādītās paroles?    4. Kādas ir prasības lietotāju kontu parolēm vai citiem kontu aizsardzības rīkiem?    5. Vai katram lietotājam parole ir obligāti jāmaina ne vēlāk kā pēc 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā?    6. Vai lietotājam tiek nodrošināts, ka lietotāja parole jāizvēlas tā, lai tā nesakristu ne ar vienu no piecām iepriekšējām lietotāja parolēm?    7. Vai piecas secīgas reizes nepareizi ievadot lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts?    8. Vai ar sistēmas administratora kontu var piekļūt personas datiem sistēmā, izmantojot iekārtas, kas atrodas ārpus organizācijas (t.sk. pašvaldības) kontrolē esošiem resursiem, kā arī iekārtas, kas neatrodas organizācijas (t.sk. pašvaldības) valdījumā, iespējams, tikai izmantojot daudzfaktoru autentifikāciju? | 18.1.  18.2.  18.3.  18.4.  18.5.  18.6.  18.7.  18.8. |  |
| 1. Lietotāji.    1. Vai ir noteikti pienākumi lietotājiem? Kādi un kur?    2. Vai fiziski piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts vienīgi iestādes pilnvarotām personām? | 19.1.  19.2. |  |
| 1. Autentifikācija    1. Vai katrs reģistrēta lietotāja konts ir saistīts ar konkrētu fizisko personu?    2. Vai ir iestrādāti kontroles mehānismi, kas novērš iespēju reģistrētiem lietotājiem izmantot sistēmkontus?    3. Vai funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām?    4. Vai tiks izmantota daudzfaktoru autentifikācija, lai piekļūtu informācijai/personas datiem? Ja jā, sniedziet informāciju par to. | 20.1.  20.2.  20.3.  20.4. |  |
| 1. Datu izmantošanas izsekojamība.    1. Vai jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei?    2. Vai ir noteikta kārtība attiecība uz personas datu izsekojamību un sistēmas/auditācijas pierakstu pārvaldību? Ja jā, sniedziet informāciju par to. | 21.1.  21.2. |  |
| 20. Papīra dokumentu drošība. Ja papīra dokuments satur personas datus un tas tiek izmantots apstrādē, norādiet kā tie tiek drukāti, uzglabāti, iznīcināti un nodoti/saņemti. |  |  |
| 1. Darbību drošība    1. Vai plūsma starp sistēmu un tās lietotājiem, kā arī starp sistēmu un citām sistēmām tiek kontrolēta, piemēram, izmantojot ugunsmūri?    2. Vai datortīkla pakalpojumi (network services), kas netiek izmantoti sistēmas darbības nodrošināšanai, ir atslēgti?    3. Vai tiek nodrošināta sistēmas/auditācijas pierakstu satura plānveida uzraudzība un analīze, lai konstatētu incidentus?    4. Cik ilgi tiks saglabāti auditācijas/sistēmas pieraksti? Norādiet noteikta termiņa nepieciešamības pamatojumu. Norādiet, kas glabās iepriekš minētos pierakstus.    5. Vai sistēmas/ auditācijas pierakstos būs ietverta informācija par lietotāja pieslēgšanos vai atslēgšanos no sistēmas, lietotāja veikto datu atlasi, visām lietotāja veiktajām darbībām (apstrādi) ar personas datiem, kā arī lietotāja konta izveidi, grozīšanu vai dzēšanu, fiksējot notikuma laiku, kas sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC), interneta protokola adresi, no kuras veikta darbība, aprakstu, kā arī informāciju par darbības iniciatoru – identifikatoru, pieslēguma metadatus?    6. Vai sistēmas lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu?    7. Vai tiek īstenota politika, lai samazinātu risku iespējamību un ietekmi uz resursiem, kas atbalsta (jeb ar kuriem apstrādā) personas datus? | 22.1.  22.2.  22.3.  22.4.  22.5.  22.6.  22.7. |  |
| 1. Vai un kā ir nodrošināta ļaunprātīgas programmatūras ietekmes[[7]](#footnote-8) samazināšana? |  |  |
| 1. Vai un kā tiek nodrošināta tīmekļa vietnes, kam ir saistība ar Projektu un personas datu apstrādi, drošība[[8]](#footnote-9). Ja attiecas. |  |  |
| 1. Vai pirms jaunas sistēmas pieņemšanas ekspluatācijā sistēmai tiks veikti ielaušanās testi un vai ielaušanās testus neveiks juridiska persona vai institūcijas darbinieki, kuri piedalījušies sistēmas izstrādē? Ja jā, kas tos veiks un kad, vai rezultāti tiks dokumentēti. |  |  |
| 1. Rezerves kopijas.[[9]](#footnote-10)    1. Vai un kā tiks veidotas sistēmas rezerves kopijas?    2. Vai ir noteikta dokumentēta kārtība rezerves kopiju veidošanai? | 26.1.  26.2. |  |
| 1. IKT resursu tehniskā apkalpošana    1. Vai ir izstrādāta IKT resursu tehniskās apkalpošanas kārtība, procedūras, instrukcijas? Norādiet dokumenta nosaukumu, datumu.    2. Vai IKT resursu tehniskās apkalpošanas kārtība ir izstrādātā saskaņā ar sistēmas darbības atjaunošanas plānu?    3. Vai pastāv politikas, kurās aprakstīts, kā tiek pārvaldīta aparatūras fiziskā apkalpošana, norādot, vai tas notiek uz līguma pamata?    4. Vai pastāv politikas, kurās aprakstīts, kā tiek īstenotas izmaiņas aparatūras, programmu konfigurācijā? Kā tiek nodrošināta konfigurācijas parametru uzraudzība un kontrole? Vai ir Sistēmas arhitektūrā un uzturēšanas procesos iestrādātas preventīvās, detektīvās un reaktīvās kontroles (security by design)?    5. Vai attālināta IKT resursu pārvaldība ir atļauta un saskaņā ar kādiem noteikumiem? Norādiet, vai bojātās iekārtas tiek pārvaldītas īpašā veidā?    6. Vai tiek nodrošināta kārtība, kurā sistēmas drošību ietekmējošu konfigurācijas parametru apstrādi iespējams veikt tikai iesaistot divus vai vairāk priviliģētos lietotājus, un tādā veidā preventīvi nepieļautu viena priviliģētā lietotāja pilnīgu kontroli?    7. Vai ir izstrādāta kārtība, kādā tiek atklāti trūkumi, nepilnības sistēmā, IKT resursos un savlaicīgi plānoti pasākumi trūkumu, nepilnību novēršanai?    8. Vai veidojot lietotāju kontus dažādu tehnoloģisku procesu veikšanai, piemēram, rezerves kopēšanai, IKT resursu turētājs kontam piešķiramās privilēģijas ierobežo tikai līdz procesa veikšanai nepieciešamajām? | 27.1.  27.2.  27.3.  27.4.  27.5.  27.6.  27.7.  27.8. |  |
| 1. Vai tiks izmantoti mākoņdatošanas pakalpojumi? |  |  |
| 1. Tīkla drošība    1. Vai piekļuve tīkla resursiem tiek regulēta, izmantojot piemēram ugunsmūri?    2. Atkarībā no tīkla veida, kurā tiek veikta informācijas resursu apstrāde (izolēts, privāts tīkls vai internets), norādiet, ugunsmūra sistēmas, ielaušanās atklāšanas sistēmas vai citas aktīvās vai pasīvās ierīces, kuras nodrošina tīkla drošību. | 29.1.  29.2. |  |
| 1. Fiziskā piekļuves kontrole. Norādiet vai un kā notiks?    1. Vai ir noteiktas politikas, kas nodrošina fizisko drošību (zonējums, apmeklētāju pavadīšana, caurlaides nēsāšana, aizslēgtas durvis un tā tālāk).    2. Vai fiziskas ielaušanās gadījumā ir spēkā brīdināšanas procedūras? | 30.  30.1.  30.2. |  |
| 1. Tīkla aktivitātes pārraudzība. Vai un ar kādiem līdzekļiem[[10]](#footnote-11) tiek uzraudzītas tīklā veiktās aktivitātes? |  |  |
| 1. Aparatūras (tehnisko resursu) drošība    1. Vai ir izstrādāts IKT resursu atjaunošanas, nomaiņas plāns?    2. Norādiet šeit kontroles, kas attiecas uz serveru un citu IKT resursu, kur atradīsies personas dati, fizisko drošību (droša glabāšana, drošības kabeļi, konfidencialitātes filtri, droša dzēšana pirms nodošanas metāllūžņos u.c). | 32.1.  32.2. |  |
| 1. Izvairīšanās no riska avotiem.    1. Vai un kā notiks?    2. Vai pastāv dokumentācija par kritisko resursu atrašanās zonu, kurai nevajadzētu būt pakļautai vides faktoru ietekmei (applūšanas zona, ķīmiskās rūpniecības tuvums, zemestrīce vai vulkāna zona utt.)? Norādiet, vai tajā pašā zonā tiek uzglabāti bīstamie produkti. | 33.1.  33.2. |  |
| 1. Aizsardzība pret riskiem, kas nav saistīti ar cilvēkiem.    1. Vai pastāv politika, kas apraksta ugunsgrēku novēršanas, atklāšanas un apkarošanas līdzekļus?    2. Vai pastāv politika, kas apraksta līdzekļus, lai novērstu ūdens bojājumus?    3. Vai pastāv politika, kas apraksta energoapgādes piegādes un to pārtraukumu uzraudzības līdzekļus? | 34.1.  34.2.  34.3. |  |
| 1. Attiecības ar trešajām pusēm    1. Vai pastāv politika un procesi, kas mazina risku, ka trešo personu likumīga piekļuve personas datiem var radīt risku datu subjektu tiesībām un privātumam?    2. Vai un kā tiek uzraudzīta un kontrolēta piekļuve personas datiem, sistēmai, IKT resursam, ja tiem piekļūst trešās personas? | 35.1.  35.2. |  |
| 1. Uzraudzība   Vai pastāv politika un procesi, lai iegūtu pārvaldību, kas spēj pārvaldīt un kontrolēt tajā esošo personas datu aizsardzību? |  |  |
| 1. Vai pirms Projekta nodošanas ekspluatācijā tiks veikta drošības atbilstības pārbaude? Pozitīvas atbildes gadījumā, norādiet pārbaudes norises kārtību. |  |  |
| 1. Vai izmantosiet ārējās informācijas sistēmas, kas būs savienotas ar organizācijas (t.sk. pašvaldības) informācijas sistēmām? Pozitīvas atbildes gadījumā, kāda ir kārtība un nosacījumi, saskaņā ar kuriem izveidosiet sadarbību ar citām organizācijām? |  |  |
| 1. Kādas tehnoloģijas un rīki tiks izmantoti, lai savienotu sistēmas? |  |  |
| 1. Vai informācijas sistēmām vai personas datiem varēs piekļūt attālināti? Pozitīvas atbildes gadījumā, kāda ir attālinātas piekļuves procedūra un nosacījumi. |  |  |
| 1. Vai tiks izmantoti tīkla pastāvīgie VPN savienojumi? Ja jā, vai:   41.1. tie tiks uzskaitīti, norādot to izveidošanas mērķi, organizācijas un mērķa IP adreses, portus, tīkla protokolus, sistēmas, kuru darbība saistīta ar VPN savienojumu un par VPN savienojumu atbildīgā persona?  41.2. Vai tiks uzskaitīti VPN savienojumu lietotāji, mērķi, kuru sasniegšanā nepieciešams lietot VPN savienojumu? | 41.  41.1.  41.2. |  |
| 1. Vai ir noteikta kārtība ārējo atmiņas ierīču pārvaldībai un lietošanai, kas attiecas uz Projektā apstrādātiem personas datiem?? Ja attiecas. |  |  |
| 1. Vai ir izstrādāta incidentu pārvaldības kārtība un procedūras, kas attiecas uz Projektā apstrādātiem personas datiem? |  |  |
| 1. Vai ir izstrādāta kārtība atklāto trūkumu (problēmu) novēršanai, kas attiecas uz Projektā apstrādātiem personas datiem? |  |  |
| 1. Vai ir izstrādāti lietošanas noteikumi attiecībā uz konkrēto resursu/Projektu? |  |  |
| 1. Vai institūcija, slēdzot līgumu par informācijas un komunikācijas tehnoloģiju sistēmu izstrādi, ieviešanu vai uzturēšanu, ir noteikusi atbildīgo personu, kas uzrauga informācijas un komunikācijas tehnoloģiju sistēmu izstrādi, ieviešanu un uzturēšanas ārpakalpojuma līguma izpildi? |  |  |
| 1. Vai sistēmā tiks nodrošināta pieejamo programmatūras atjauninājumu uzlikšana un iepriekš izvērtēta to nepieciešamība? |  |  |
| 1. Ja sistēma tiks nodrošināta elektroniskā pasta saņemšanu no ārējiem resursiem, vai ienākošās saziņas apstrādē notiks vismaz atbilstoši e-pastu autentifikācijas protokola (DMARC[[11]](#footnote-12)) prasībām, un tiks ieviesta e-pasta apstrāde atbilstoši sūtītāja domēna vārda DMARC politikai, atskaites ģenerēšana un nosūtīšana DMARC konfigurācijā norādītajam kontaktam? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju ir vai tiek plānots ietvert ārpakalpojuma sniedzēja pienākums nekavējoties ziņot par informācijas tehnoloģiju drošības incidentu un veikt visas tā novēršanai nepieciešamās darbības? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju ir ietverts vai tiek plānots ietvert ārpakalpojuma sniedzēja pienākums informēt par apakšuzņēmēju un viņa atbilstību Ministru kabineta 2015. gada 28. jūlija noteikumiem Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" un ārpakalpojuma līgumā noteiktajām drošības prasībām? |  |  |
| 1. Vai līgumā ar ārpakalpojumu sniedzēju tiks ietverts saņemamā ārpakalpojuma apraksts? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju tiks ietvertas precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju tiks ietvertas institūcijas tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju tiks ietvertas institūcijas tiesības iesniegt ārpakalpojuma sniedzējam pamatotu rakstisku pieprasījumu nekavējoties izbeigt ārpakalpojuma līgumu, ja institūcija konstatējusi, ka ārpakalpojumu sniedzējs nepilda ārpakalpojuma līgumā noteiktās prasības attiecībā uz ārpakalpojuma apjomu vai kvalitāti? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju tiks ietverts ārpakalpojuma sniedzēja pienākums nodrošināt institūcijai iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju tiks ietverts ārpakalpojuma sniedzēja pienākums informēt par apakšuzņēmēju un viņa atbilstību šajos noteikumos un līgumā noteiktajām drošības prasībām? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju tiks ietvertas piekļuves prasības datiem un to uzglabāšanai, kā arī pienākumu piegādātājam pēc līguma termiņa beigām dzēst viņa rīcībā nonākušos datus, izņemot gadījumu, ja atkārtoti tiks slēgts līgums ar to pašu pakalpojuma sniedzēju par to pašu līguma priekšmetu. |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju ir ietvertas vai tiek plānots ietvert normatīvajos aktos noteiktās un citas institūcijas vadītāja identificētās sistēmai veicamās drošības pārbaudes? |  |  |
| 1. Vai līgumā ar ārpakalpojuma sniedzēju ir ietvertas vai tiek plānots ietvert piekļuves prasības datiem un to uzglabāšanai? |  |  |
| 1. Vai iegādājoties pakalpojumu, programmatūru (vai iekārtu), iepirkuma specifikācijā un līgumā ir ietverts vai tiek plānots ietvert pienākumu pakalpojuma sniedzējam un produkta ražotājam līguma darbības laikā informēt vai publicēt informāciju par atklātajām informācijas un komunikācijas tehnoloģiju produkta vai pakalpojuma ievainojamībām, to novēršanas pasākumiem un termiņiem? |  |  |
| 1. Vai ārpakalpojuma sniedzējs būs : |  |  |
| * 1. juridiska persona, kas: |  |  |
| 62.1.1. reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī?  62.1.2. patiesais labuma guvējs būs NATO, Eiropas Savienības, Eiropas Ekonomikas zonas valsts pilsonis vai Latvijas Republikas nepilsonis?  62.1.3. pakalpojuma nodrošināšanai izmantoto programmatūru vai iekārtu ražotājs būs juridiska persona, kas reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, vai fiziska persona, kas ir Latvijas Republikas valstspiederīgais, NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas valsts pilsonis? |  |  |
| * 1. fiziska persona, kas ir NATO, Eiropas Savienības, Eiropas Ekonomikas zonas valsts pilsonis vai Latvijas Republikas nepilsonis? |  |  |
| * 1. Vai iegādājoties pakalpojumu, programmatūru vai iekārtu iepirkuma specifikācijā un līgumā tiks iekļauts pienākums pakalpojuma sniedzējam un produkta ražotājam līguma darbības laikā informēt vai publicēt informāciju par atklātajām informācijas un komunikācijas tehnoloģiju produkta vai pakalpojuma ievainojamībām, to novēršanas pasākumiem un termiņiem? |  |  |
| 1. Vai ir identificējami vēl kādi citi riski, kas netika iekļauti iepriekšējās atbildēs? |  |  |

|  |  |
| --- | --- |
| **Novērtējuma veicējs:** |  |
| **Novērtējuma veikšanas datums:** |  |
| **Pašvaldības struktūrvienība/iestāde:** |  |
| **Ziņas par trūkumu novēršanu un termiņš** |  |
| **Iepazīstinātas ar novērtējuma rezultātu sekojošas personas:** |  |
| **Novērtējuma veicēja paraksts:** |  |

1. Programmatūra, aparatūra, iekārtas, operētājsistēmas, biznesa lietojumprogrammas, biroja programmatūra, datu bāzu pārvaldības sistēmas, tīkli, tīklam pieslēgto iekārtu pārvaldības, darbības novērošanas un lietotāju administrēšanas un autorizācijas programmas, loģiskās aizsardzības programmas (antivīrusu programmas, ugunsmūra programmas u.c. [↑](#footnote-ref-2)
2. Tas ir līdzeklis, kas tiek īstenots, lai nodrošinātu uzglabāto datu konfidencialitāti (datu bāzē, failos, u.c), kā arī vai ir noteikta šifrēšanas atslēgu pārvaldīšanas kārtība. [↑](#footnote-ref-3)
3. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\_lv.pdf [↑](#footnote-ref-4)
4. Personas datu apstrāde tādā veidā, ka personas datus vairs nevar attiecināt uz konkrētu datu subjektu, neizmantojot papildu informāciju, ar nosacījumu, ka šādu papildu informāciju glabā atsevišķi un uz to attiecas tehniski un organizatoriski pasākumi, lai nodrošinātu, ka personas dati netiek attiecināti uz identificētu vai identificējamu fizisku personu. Pseidonimizācija samazina datu kopas saistību ar datu subjekta sākotnējo identitāti; kā tāds, tas ir noderīgs drošības pasākums, bet ne anonimizācijas metode. [↑](#footnote-ref-5)
5. Datu nodalīšana no citas informācijas ieviešana palīdz mazināt iespējamību, ka personas datus var savstarpēji saistīt un, ka var notikt personas datu aizsardzības pārkāpums. Piemēram, nosakot personas datus, kas ir noderīgi tikai noteiktam procesam, un tos loģiski atdalot. [↑](#footnote-ref-6)
6. Līdzekļi, kas tiek īstenoti, lai ierobežotu risku, ka nepilnvarotas personas elektroniski piekļūs personas datiem, tai skaitā:

   - lietotāju profilu pārvaldīšana, nodalot uzdevumus un atbildības jomas (vēlams centralizēti), lai ierobežotu piekļuvi personas datiem tikai autorizētiem lietotājiem, piemērojot principu – zināt tikai to, kas nepieciešams;

   - atsaukt darbinieku, līgumslēdzēju pušu un citu trešo personu tiesības, kad viņiem vairs nav tiesību piekļūt telpām vai resursiem vai kad beidzas viņu darba līgums. [↑](#footnote-ref-7)
7. Ieviestas kontroles, ko ievieš darbstacijās un serveros, lai tos aizsargātu pret ļaunprātīgu programmatūru, piekļūstot mazāk drošiem tīkliem. [↑](#footnote-ref-8)
8. OWASP noteikto risku un ieteikumu ieviešana tīmekļa vietņu nodrošināšanai. [↑](#footnote-ref-9)
9. Politikas un līdzekļi, kas tiek īstenoti, lai nodrošinātu personas datu pieejamību un/vai integritāti, vienlaikus saglabājot to konfidencialitāti. [↑](#footnote-ref-10)
10. Novēro ielaušanās atklāšanas sistēmas un ielaušanās novēršanas sistēmas, lai reālā laikā analizētu tīklu (vadu tīklus, Wi-Fi, radioviļņus, optisko šķiedru utt.) un atklātu aizdomīgas darbības, kas liecina par kiberuzbrukuma scenāriju. [↑](#footnote-ref-11)
11. Domain-based Message Authentication, Reporting and Conformance [↑](#footnote-ref-12)